أمن المعلومات

GS224-8

هجوم تعطيل الخدمة (DoS)

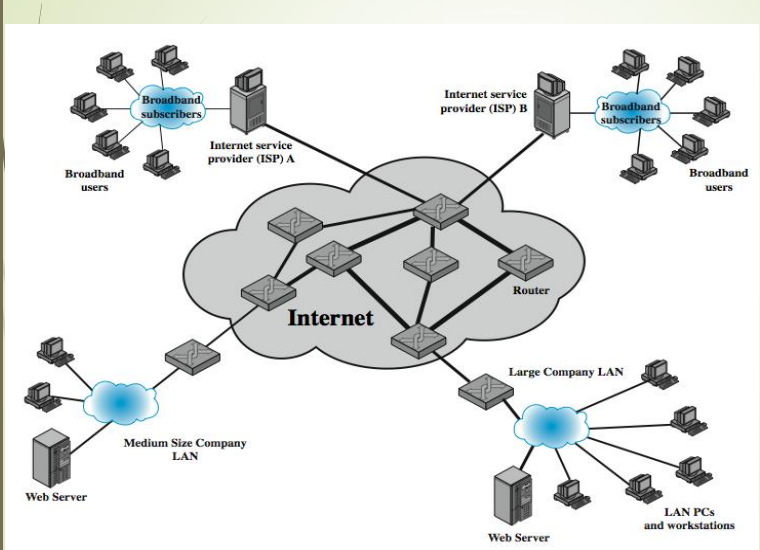
- تعطيل الخدمة (DoS): هو إجراء يمنع أو يضعف الاستخدام المصرح به للشبكات أو الأنظمة أو التطبيقات عن طريق استنفاد الموارد مثل وحدات المعالجة المركزية او الذاكرة او عرض النطاق الترددي او مساحة القرص.
- الهجمات: (التحميل الزائد أو طلبات خدمة غير صالحة تستهلك موارد كبيرة).
  - عرض النطاق الترددي للشبكة - يتعلق بسعة روابط الشبكة التي تربط الخادم بالروابط الاوسع لنظام الإنترنت.
  - موارد النظام - تهدف عادةً إلى زيادة التحميل أو تعطيل برامج مناولة الشبكة.
  - موارد التطبيق - تهدف إلى انهاك لقدرات الخادم والحد من قدرته على الاستجابة لطلبات المستخدمين الآخرين.
- كانت هجمات تعطيل الخدمة مشكلة لسنوات عديدة. أفاد استطلاع مكتب التحقيقات الفدرالي لجرائم الحاسوب والأمن لعام 2006 أن 25٪ من المستطلعين قد تعرضوا لشكل من أشكال هجوم الحرمان من الخدمة في الأشهر 12 الماضية. وقد تفاوتت هذه القيمة بين 25٪ و 40٪ خلال السنوات الثماني الماضية من الدراسات الاستقصائية.

هجوم تعطيل الخدمة التقليدي

- الفيضان بأمر (ping).
  - الهدف من هذا الهجوم هو التغلب على قدرة اتصال الشبكة بالمؤسسة المستهدفة.
  - يمكن معالجة حركة المرور من خلال روابط ذات سعة أعلى على المسار ، ولكن يتم تجاهل الحزم مع انخفاض السعة.
- يتم تحديد مصدر الهجوم بوضوح ما لم يتم استخدام عنوان مخادع.
- يتأثر أداء الشبكة بشكل ملحوظ.

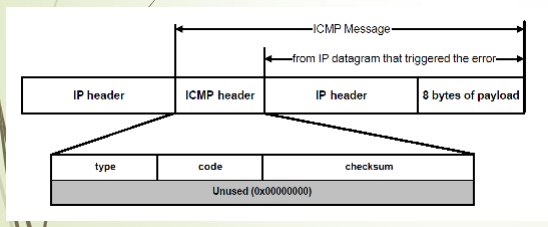
هجوم تعطيل الخدمة التقليدي

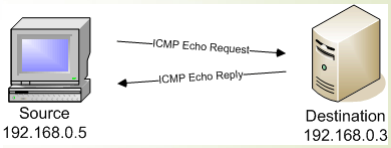
- على سبيل المثال ، في الشبكة الموضحة في الشكل ، قد يستخدم المهاجم خادم الويب للشركة الكبيرة لاستهداف شركة متوسطة الحجم ذات اتصال بشبكة منخفض السعة.



بروتوكول رسالة التحكم في الانترنت (ICMP)

- يعد بروتوكول رسالة التحكم في الإنترنت (ICMP) أحد بروتوكولات بروتوكول الانترنت (IP) الرئيسية ؛ ويتم استخدامه بواسطة أجهزة الشبكة ، مثل أجهزة التوجيه ، لإرسال رسائل تشير للخطأ (على سبيل المثال ، الخدمة المطلوبة غير متوفرة أو تعذر الوصول إلى المضيف أو جهاز توجيه).





يجب أن يستجيب المضيف لجميع طلبات الصدى بجواب الصدى الذى يحتوي على البيانات الدقيقة الواردة في رسالة الطلب

انتحال عنوان المصدر

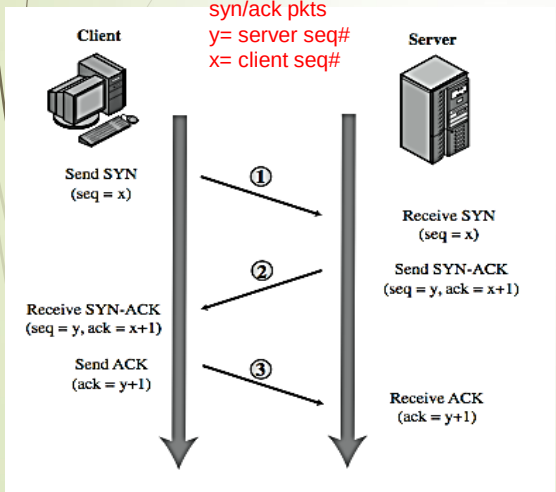
- من الخصائص الشائعة للحزم المستخدمة في العديد من أنواع هجمات تعطيل الخدمة استخدام عناوين مصدر مزورة. يُعرف هذا باسم **انتحال عنوان المصدر**.
- في حال الحصول على امتيازات الكافية للوصول الى برنامج مناول الشبكة على نظام الحاسب ، فمن السهل إنشاء حزم بعنوان مصدر مزور (وفي الواقع أي سمة أخرى مرغوبة).
- عند التمكن من الوصول إلى واجهة الشبكة ، يقوم المهاجم بإنشاء كميات كبيرة من الحزم. سيكون لكل منها النظام الهدف كعنوان الوجهة ، ولكن مستخدمة عناوين مصدر يتم اختيارها عشوائيًا وعادةً ما تكون مختلفة لكل حزمة. وسوف تتدفق هذه الحزم على نفس المسار من المصدر نحو النظام الهدف.
- نفس الازدحام سيتم على جهاز التوجيه المرتبط بالمسار النهائي ذي السعة المنخفضة. ومع ذلك ، فإن حزم الاستجابة والتي تم إنشاؤها استجابة للحزم التي وصلت الى النظام المستهدف ، لن تنعكس مرة أخرى الى النظام المصدر. بدلاً من ذلك سيتم نشرها عبر الإنترنت لجميع عناوين المصادر المزورة المختلفة.
- قد تتوافق بعض هذه العناوين مع أنظمة حقيقية ، وقد لا يتم استخدام البعض الآخر أو لا يمكن الوصول إليها. بالإضافة إلى ذلك ، فإن استخدام حزم ذات عناوين مصدر مزورة يعني صعوبة التعرف على نظام المهاجم.
- حزم الهجوم تبدو و كأنها قد أنشأت من عناوين منتشرة عبر الإنترنت. ومن ثم فإن مجرد فحص رأس كل حزمة لا يكفي لتحديد مصدرها. وبدلاً من ذلك ، يجب تحديد تدفق الحزم بشكل معين عبر أجهزة التوجيه على طول المسار من المصدر إلى النظام الهدف.

هجوم انتحال (SYN)

- هجوم تعطيل للخدمة شائع.
- يستهدف هذا الهجوم قدرة خادم الشبكة على الاستجابة لطلبات اتصال (TCP) عن طريق تجاوز سعة الجداول المستخدمة لإدارة مثل هذه الاتصالات.
- هذا يعني أن طلبات الاتصال المستقبلية من المستخدمين الشرعيين تفشل ، مما يمنعهم من الوصول إلى الخادم. (تم رفض وصول المستخدمين الشرعيين إلى الخادم).
- ومن ثم هجوم على موارد النظام ، وتحديداً برنامج مناول الشبكة في نظام التشغيل.

أسلوب اتصال (TCP)

لفهم عمل هذه الهجمات نحتاج إلى مراجعة الاتصال ثلاثي الاتجاهات الذي يستخدمه بروتوكول (TCP) لإنشاء اتصال (الشكل التالي).



- يبدأ نظام العميل طلب اتصال (TCP) عن طريق إرسال حزمة (SYN) إلى الخادم. يحدد هذا عنوان العميل ورقم المنفذ ، ويقدم رقم تسلسل أولي.
- يسجل الخادم جميع التفاصيل المتعلقة بهذا الطلب في جدول معروف باتصالات (TCP)، ثم يستجيب للعميل بحزمة (SYN-ACK) وتتضمن هذه رقم تسلسل للخادم ، ويزيد رقم تسلسل العميل لتأكيد استلام حزمة (SYN) .

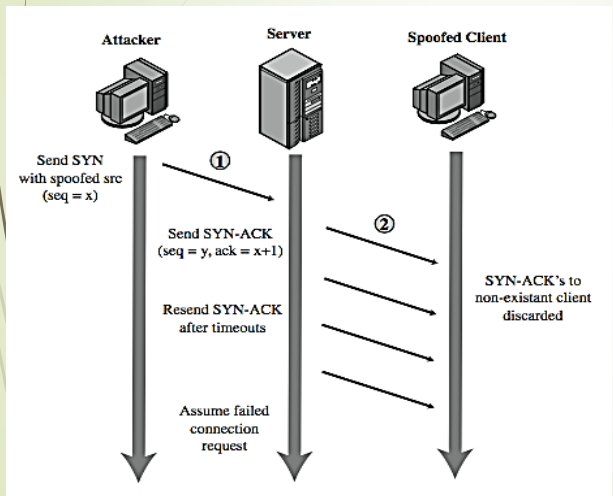
أسلوب اتصال (TCP)

- بمجرد أن يتلقى العميل ذلك ، فإنه يرسل حزمة (ACK) إلى الخادم برقم تسلسل خادم متزايد ، ويضع علامة على الاتصال على أنه تم إنشاؤه.
- وبالمثل ، عندما يتلقى الخادم حزمة (ACK) هذه ، فإنه يشير أيضًا إلى الاتصال على أنه تم إنشاؤه ويمكن لأي من الطرفين بعد ذلك متابعة نقل البيانات. من الناحية العملية يفشل هذا التبادل المثالي أحيانًا. يتم نقل هذه الحزم باستخدام (IP) ، وهو بروتوكول شبكة غير موثوق به وإن كان هو الأفضل، فقد يتم فقد أي من الحزم أثناء النقل نتيجة الازدحام على سبيل المثال.
- ومن ثم يتتبع كل من العميل والخادم الحزم التي أرسلوها ، وإذا لم يتم تلقي استجابة في وقت معقول ، فسيعيد إرسال هذه الحزم. نتيجة لذلك ، يعد بروتوكول (TCP) بروتوكول نقل موثوقًا به ، وأي تطبيقات تستخدمه لا تحتاج إلى الاهتمام بمشاكل الحزم المفقودة أو المعاد ترتيبها.

هجوم انتحال (SYN)

يستغل هجوم انتحال (SYN) هذا السلوك على نظام الخادم المستهدف.

- ينشئ المهاجم عددًا من حزم طلبات اتصال (SYN) بعناوين مصدر مزورة.
- لكل منها ، يسجل الخادم تفاصيل طلب اتصال (TCP) ، ويرسل حزمة (SYN-ACK) إلى عنوان المصدر المطالب به ، كما هو موضح في الشكل.



الافتراض: تنجح معظم الاتصالات
وبالتالي يتم مسح الجدول بسرعة

هجوم انتحال (SYN)

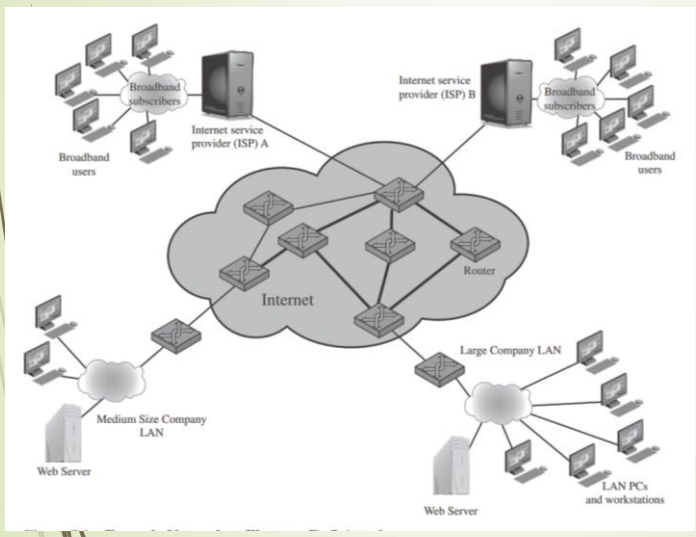
- سيقوم الخادم بإعادة إرسال حزمة (SYN-ACK) عدة مرات قبل الافتراض أخيرًا أن طلب الاتصال قد فشل ، وحذف المعلومات المحفوظة المتعلقة به.
- يتم تحديد حجم هذا الجدول عادةً على افتراض أن معظم طلبات الاتصال تنجح بسرعة ، وأنه يمكن معالجة عدد معقول من الطلبات في وقت واحد.
- ومع ذلك ، في هجوم انتحال (SYN) ، يوجه المهاجم عددًا كبيرًا جدًا من طلبات الاتصال المزورة على الخادم المستهدف. تملأ هذه بسرعة جدول اتصالات (TCP) على الخادم.
- بمجرد امتلاء هذا الجدول ، يتم رفض أي طلبات مستقبلية ، بما في ذلك الطلبات المشروعة من مستخدمين آخرين. مع انتهاء مهلة مدخلات الجدول ستتم إزالتها مما يؤدي في حالة الاستخدام العادي للشبكة إلى تصحيح مشكلات تجاوز سعة التخزين المؤقتة.
- ومع ذلك ، إذا احتفظ المهاجم بتدفق كمية كافية من الطلبات المزورة ، فسيكون هذا الجدول ممتلئًا باستمرار وسيتم قطع الخادم بشكل فعال عن الإنترنت ، ولن يتمكن من الاستجابة لمعظم طلبات الاتصال المشروعة.

هجوم انتحال (SYN) : مصادر الهجوم

- من أجل زيادة استخدام جدول اتصالات (TCP) ، يرغب المهاجم بشكل مثالي في استخدام العناوين التي لن تستجيب (SYN-ACK) بالرد (RST) .يمكن القيام بذلك
  - عن طريق التحميل الزائد على المضيف الذي يمتلك عنوان المصدر المخادع المختار ، أو
  - ببساطة عن طريق استخدام مجموعة واسعة من العناوين العشوائية. في هذه الحالة ، يعتمد المهاجم على حقيقة وجود العديد من العناوين غير المستخدمة على الإنترنت. وبالتالي ، فإن نسبة معقولة من العناوين التي تم إنشاؤها عشوائيًا لن تتوافق مع مضيف حقيقي.
- يوجد فرق كبير في حجم حركة مرور الشبكة بين هجوم انتحال (SYN) وهجوم الاغراق الأساسي. يمكن أن يكون الحجم الفعلي لحركة مرور (SYN) منخفضًا نسبيًا، ولا يقترب من السعة القصوى للارتباط بالخادم ويجب ببساطة أن يكون مرتفعًا بدرجة كافية لإبقاء جدول اتصالات (TCP) ممتلئًا. على عكس هجوم الإغراق ، فإن هذا يعني أن المهاجم لا يحتاج إلى اتصال بشبكة كبير الحجم.

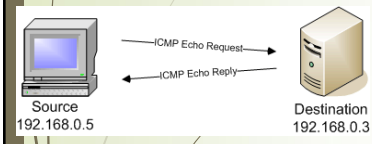
هجوم انتحال (SYN) : مصدر الهجوم

- في الشبكة الموضحة في الشكل ، يمكن للمؤسسة متوسطة الحجم ، أو حتى مستخدم منزلي واسع النطاق ، مهاجمة خادم شركة كبيرة بنجاح باستخدام هجوم انتحال (SYN).



أنواع هجوم الإغراق (Flooding)

- تتخذ هجمات الاغراق أشكالًا متنوعة ، بناءً على بروتوكول الشبكة المستخدم لتنفيذ الهجوم. تستخدم هجمات الإغراق الشائعة أيًا من أنواع حزم (ICMP) أو (UDP) أو (TCP SYN).
- الهدف: زيادة الحمل على سعة الشبكة على بعض روابطها لخادم ما.
- يمكن استخدام أي نوع من حزم الشبكة تقريبًا.
- هجوم الإغراق باستخدام (ICMP)
  - يستخدم حزمة (ICMP) ، مثل حزم صدى طلب (ICMP) في الإغراق باستخدام (ping).
  - تم اختيار هذا النوع من حزم (ICMP) نظرًا لأنه تقليديا يسمح مسؤولي الشبكة بمثل هذه الحزم في شبكاتهم.
  - في الآونة الأخيرة ، قامت العديد من المنظمات بتقييد قدرة هذه الحزم على المرور عبر جدران الحماية الخاصة بها.
  - ردًا على ذلك ، بدأ المهاجمون في استخدام أنواع أخرى من حزم (ICMP) نظرًا لأنه يجب معالجة بعض هذه العناصر للسماح بالتشغيل الصحيح لبروتوكول (TCP / IP)، فمن المرجح أن يتم السماح بها من خلال جدار حماية المؤسسة.



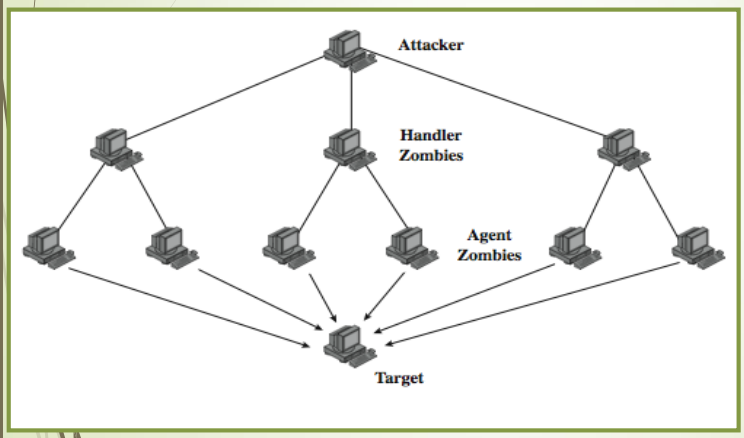
أنواع هجوم الإغراق (Flooding)

- هجوم الإغراق باستخدام (UDP) ، (أحد البدائل لاستخدام حزم (ICMP) هو:
  - استخدم حزم (UDP) موجهة إلى بعض أرقام المنافذ (منافذ العشوائية) ، وبالتالي الخدمة النشطة على النظام المستهدف (حتى في حالة عدم توفر خدمة ، يحقق المهاجم هدفه).
  - عادة ما تستخدم عناوين مصادر مزيفة إذا تم إنشاء الهجوم باستخدام نظام واحد ، ولنفس الأسباب مثل هجمات (ICMP).
- هجوم الإغراق باستخدام (TCP SYN)
- بديل آخر هو إرسال حزم (TCP) إلى النظام المستهدف.
- على الأرجح ستكون هذه طلبات اتصال (TCP) عادية ، مع عناوين مصدر حقيقية أو مزيفة.
- في هذه الحالة ، يكون هدف الهجوم هو الحجم الإجمالي للحزم ، بدلاً من استهداف برامج النظام تحديدًا.
- هذا هو الفرق بين هجوم انتحال (SYN) وهجوم إغراق (SYN) .

هجوم تعطيل الخدمة الموزع (DDos)

- كل هجومات الإغراق السابقة محدودة في الحجم الإجمالي لحركة المرور التي يمكن إنشاؤها إذا تم استخدام نظام واحد فقط لشن الهجوم. (لها حجم محدود إذا تم استخدام مصدر واحد).
- تسمح الأنظمة المتعددة بحجم مرور أعلى بكثير لتشكيل هجوم تعطيل الخدمة موزع (DDoS).
- باستخدام أنظمة متعددة ، يمكن للمهاجم زيادة حجم حركة المرور التي يمكن إنشاؤها بشكل كبير. لا يلزم أن يكون كل نظام من هذه الأنظمة قويًا بشكل خاص ، أو على ارتباط عالي السعة ، لكن ما لا يملكه بشكل فردي فإنهم يعوضون عنه بأعدادهم الكبيرة.
- هذه الأنظمة تخترق عادةً محطات عمل المستخدم أو أجهزة الحاسوب الشخصي.
  - استخدم المهاجم بعض العيوب المعروفة في نظام التشغيل أو في بعض التطبيقات الشائعة للوصول إلى هذه الأنظمة ولتثبيت برامجهم الخاصة عليها. تُعرف هذه الأنظمة باسم "الزومبي".
  - بمجرد تثبيت برامج "الباب الخلفي" المناسبة على هذه الأنظمة ، أصبحت بالكامل تحت سيطرة المهاجم. يمكن إنشاء مجموعات كبيرة من هذه الأنظمة تحت سيطرة مهاجم واحد ، لتشكيل "بوت نت" بشكل جماعي.

هيكلية التحكم في هجوم تعطيل الخدمة الموزع (DDos)



- بينما يمكن للمهاجم أن يأمر كل وكيل (زومبي) على حدة ، لكن يتم استخدام التسلسل الهرمي للتحكم بشكل عام. يعمل عدد صغير من الأنظمة كمعالجات تتحكم في عدد أكبر بكثير من الأنظمة الوكيلة ، كما هو موضح في الشكل.

المهاجم يرسل أمر واحد الى مناولى الوكلاء (زومبي)
و من ثم يمرره المناول الى مناولي عملاء اخرين

هيكلية التحكم في هجوم تعطيل الخدمة الموزع (DDos)

- هناك عدد من المزايا لهذا الترتيب.
  - يمكن للمهاجم إرسال أمر واحد إلى مناول ، والذي يقوم بعد ذلك بإعادة توجيهه تلقائيًا إلى جميع العملاء الخاضعين لسيطرته.
  - يمكن أيضًا استخدام أدوات العدوى الآلية للبحث عن أنظمة الزومبي المناسبة والتغلب عليها.
  - بمجرد تحميل برنامج الوكيل على نظام تم اختراقه حديثًا ، يمكنه الاتصال بواحد أو أكثر من المناولين لإخطارهم تلقائيًا بتوافره.
  - وبهذه الوسيلة ، يمكن للمهاجم أن ينمي تلقائيًا "شبكات روبوت" مناسبة.
- أفضل دفاع ضد كونك مشاركًا غير مقصود في هجوم (DDoS) هو منع اختراق أنظمتك. بالنسبة لهدف هجوم (DDoS) ، تكون الاستجابة مماثلة لأي هجوم إغراق ، ولكن بحجم وتعقيد أكبر.

الهجمات المعتمدة في برتوكول (HTTP)

- محاولات الاحتكار عن طريق إرسال طلبات (HTTP) التي لا تكتمل أبدًا.
- يستهلك في النهاية سعة اتصال خادم الويب.
- يستخدم حركة مرور (HTTP) مشروعة
- تبدأ الروبوتات من رابط (HTTP) معين وتتبع جميع الروابط الموجودة على موقع الويب المقدم بطريقة متكررة.
- تعتم أنظمة كشف التطفل والوقاية الحالية على التوقيعات و الانماط لاكتشاف الهجمات بشكل عام .

خطوط دفاع ضد هجمات (DDoS)

- منع الهجوم والاستباق (قبل الهجوم)
- كشف الهجمات وتصفيتها (أثناء الهجوم)
- تتبع مصدر الهجوم وتحديد هويته (أثناء الهجوم وبعده)
- رد فعل الهجوم (بعد الهجوم)

منع هجمات (DoS)

- منع عناوين ذات المصدر المزيف بواسطة أجهزة التوجيه تكون أقرب ما يمكن من المصدر.
- يمكن استخدام المرشحات للتأكد من أن المسار إلى عنوان المصدر المطالب به هو الذي تستخدمه الحزمة الحالية.
  - يجب تطبيق عوامل التصفية على حركة المرور قبل أن تغادر شبكة مزود خدمة الإنترنت أو عند نقطة الدخول إلى شبكتهم.
- استخدم برنامج مناولة اتصال (TCP) معدل.
- تشفير المعلومات الهامة بشكل مشفر في ملف تعريف ارتباط يتم إرساله كرقم التسلسل الأولي للخادم.
- يستجيب العميل الشرعي بحزمة (ACK) تحتوي على ملف تعريف ارتباط برقم التسلسل المتزايد.
- قم بإسقاط مدخلات الاتصال غير المكتمل من جدول اتصالات (TCP) عند الاغراق.

منع هجمات (DoS)

- ضبط معدل النقل على شبكات التوزيع.
- على أنواع حزم معينة ، على سبيل المثال بعض (ICMP)، بعض (UDP) ، (TCP / SYN).
- فرض قيود.
- استخدام مناول اتصال (TCP) معدل.
  - يرسل الخادم ملفات تعريف الارتباط (SYN) عندما يكون الجدول ممتلئًا (إعادة بناء بيانات الجدول من ملف تعريف الارتباط من العملاء الشرعيين).
  - إسقاط عشوائي أو انتقائي عند امتلاء الجدول.
- منع عمليات البث لبروتوكول (IP) الموجهة.
- حظر الخدمات والتركيبات المشبوهة.
- إدارة هجمات التطبيقات باستخدام شكل من أشكال الألغاز الرسومية (captcha) لتمييز الطلبات البشرية المشروعة.
- استخدم الخوادم ذات النسخ المتطابقة والنسخ المتماثل عند الحاجة إلى الأداء العالي والموثوقية.

الرد على هجمات (DoS)

- تحديد نوع الهجوم
- التقاط وتحليل الحزم
- تصميم مرشحات لمنع هجوم حركة المرور
- أو تحديد أخطاء النظام / التطبيقات وتصحيحها
- ضروري في حالة التخطيط لإجراء قانوني
- تنفيذ خطة الطوارئ
- قم بالتبديل إلى خوادم النسخ الاحتياطي البديلة (خوادم جديدة في موقع جديد بعناوين جديدة)
- تحديث خطة الاستجابة للحوادث (خطة جيدة للاستجابة للحدث)
- تفاصيل حول كيفية الاتصال بالدعم الفني لمزود خدمة الإنترنت (احصل على تدفق حزمة تتبع (ISP) مرة أخرى إلى المصدر)
- فرض تصفية حركة المرور عند بداية المسارات
- وضع تفاصيل لكيفية الرد على الهجوم
- تنفيذ مرشحات مكافحة الانتحال والبث الموجه
- من الناحية المثالية ، يكون لديك شاشات مراقبة الشبكة و نظام كشف التطفل لاكتشاف وإخطار أنماط حركة المرور غير الطبيعية على الشبكة.